CSIRT INQUEST - RFC2350

17/08/2023

TABLE DES MATIERES

1. DOCUMENT INFORMATION

This document contains a description of CSIRT-INQUEST in accordance with RFC 2350 [1] specification. It provides basic information about CSIRT-INQUEST, describes its responsibilities and services offered.

1.1. Date of last update

Version 1.1, published on 2023-08-17.

1.2. Distribution list for notifications

There is no distribution list for notifications.

Please send questions about updates to CSIRT-INQUEST team email address : csirt[at]inquest-risk.com

1.3. Locations where this document may be found

The current and latest version of this document is available on the inquest's website. Its URL is:
https://www.inquest-risk.com/app/uploads/sites/2/2023/08/rfc2350-csirt-inquest-v1.1.pdf

1.4. Authenticating this document

This document has been signed with the PGP key of CSIRT-INQUEST.
The PGP public key, ID and fingerprint are available on the inquest's website. Its URL is :
www.inquest-risk.com

1.5. Document identification

Title: « CSIRT INQUEST - RFC2350 »
Version : 1.1
Document Date : 2023-08-17
SHA-256
Expiration : this document is valid until superseded by a later version

2. CONTACT INFORMATION

2.1. Name of the team

CSIRT-INQUEST

CSIRT-INQUEST is Inquest's commercial CSIRT.

2.2. Address

CSIRT INQUEST
CAMPUS AVISO
13-15 rue Jean Jaurès
92800 PUTEAUX – France

2.3. Time zone

CET/CEST

[1] https://www.ietf.org/rfc/rfc2350.txt

2.4. Telephone number
Main number (duty office): +33 1 76 39 12 15

2.5. Facsimile Number
Not applicable

2.6. Other Telecommunication
Not applicable

2.7. Electronic mail address
If you need to notify us about an information security incident or a cyber-threat targeting or involving your company, please contact us at csirt[at]inquest-risk.com.

2.8. Public keys and encryption information
PGP is used for functional exchanges with CSIRT-INQUEST.
- User ID : CSIRT-INQUEST <csirt[at]inquest-risk.com>
- Key ID : 0xC11B8BC5
- Fingerprint: 3B53 5D16 5794 0092 B45F 64B2 7675 BDDE C11B 8BC5

The public PGP key is available at :
https://www.inquest-risk.com/app/uploads/sites/2/2022/11/CSIRT-INQUEST_public_key.asc
It can be retrieved from one of the usual public key servers.

2.9. Team members

CSIRT Director : Thibault CARRE <thibault.carre[at]inquest-risk.com>
CSIRT Deputy Director : Jean-François Vanderplancke <jf.vanderplancke[at]inquest-risk.com>

The list of the CSIRT-INQUEST's team members is not publicly available. The team consists of Inquest's IT security analysts.

2.10. Points of customer contact
CSIRT-INQUEST prefers to receive incident reports via e-mail at csirt[at]inquest-risk.com. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.
CSIRT-INQUEST's hours of operation are 7/7 24h all year long.

3. CHARTER
3.1 Mission statement
CSIRT-INQUEST is a private CSIRT team delivering security services, mainly in France and Europe.

CSIRT-INQUEST's missions cover prevention, response and recovery by:
- Helping to prevent security incidents in set up necessary protection measures;
- Detecting vulnerabilities on networks and systems;
- Managing incident response, with the support of trusted partners if necessary;

CSIRT-INQUEST strives to act according to the highest standards of ethics, integrity, honesty and professionalism and is committed to deliver a high-quality service to its constituency.

3.2 Constituency

CSIRT-INQUEST provides services to its Customers Community, who subscribed support contracts.

3.3 Sponsorship and/or affiliation

CSIRT-INQUEST is part of Inquest : https://www.inquest-risk.com/.
CSIRT-INQUEST maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis.

3.4 Authority

CSIRT-INQUEST operates within the framework of contracts, validated and signed with its customers. The team has no authority to request the performance of actions on the systems and networks on the impacted perimeters.

4. POLICIES

4.1 Types of incidents and level of support

CSIRT-INQUEST addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see 3.2).
The level of support given by CSIRT-INQUEST will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CSIRT-INQUEST's resources at the time. Depending on the security incident's type, CSIRT-INQUEST will gradually roll out its services which include incident response and digital forensics.

CSIRT-INQUEST services include reactive and proactive services :

- On-call 24 hours a day ;
- Incident response assistance and support ;
- Incident response and remediation ;
- Incident analysis and forensics ;
- Analysis of vulnerabilities and malware.

In addition, CSIRT-INQUEST liaises with insurance for insured clients.

4.2. Co-operation, interaction and disclosure of information

General incident related information such as names and technical details is not published without agreement of the named parties. If not agreed otherwise, supplied information is kept confidential. CSIRT-INQUEST will never pass information to third-parties unless required by law. Under the condition of acceptance through affected parties or authorized by law, CSIRT-INQUEST prefers to share Tactics, Techniques and Procedures for the purpose of prevention and reaction to specific incidents.

All information is passed depending on its classification and the need-to-know principle. Only the specifically relevant and anonymised extracts are passed on. CSIRT-INQUEST respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED as described by the FIRST definitions at : www.first.org/tlp/
CSIRT-INQUEST handles and processes information in secured physical and technical environments in accordance with the French state regulations for the protection of information.

4.3. Communication and authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CSIRT-INQUEST uses encryption solutions. By default, all sensitive communication to CSIRT-INQUEST should be encrypted with our public PGP key detailed in Section 2.8.

5 SERVICES

5.1. Incident response

CSIRT-INQUEST's incident response services are available on a 24/7 basis to our constituency. All information and communication technologies related incidents are evaluated. In-depth analysis is provided by technical experts.

CSIRT-INQUEST provides 2 major services in the field of Incident Response :

- Incident Coordination,
- Incident Resolution.

But before these services are performed, a first task is to perform :

- Incident Triage

5.2. Incident triage

- Collect information about the incident.
- Confirm that the described event is actually a cyber security incident and is related to our constituency.
- Determine the severity of the incident (what is the impact) and its extent (how many computers are affected).
- Decide which type of service (coordination or resolution) should be triggered.

5.3. Incident coordination

- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary and if requested by our constituency.

5.4. Incident resolution

- Performing data acquisition and analysis (hard drive and memory forensics)
- Determining the initial cause of the incident (vulnerability exploited).
- Elimination of the cause of a security incident (the vulnerability exploited) and its effects (for example, continuing access to the system by an intruder)
- Providing support for removing the vulnerability.
- Providing support for securing the system from the effects of the incident.

5.5. Proactive activities

- IS security audits (organizational audits, compliance audits, etc.);
- Search for compromises/threat hunting. CSIRT-INQUEST can conduct investigations on networks or systems, in order to search for potential compromises of these.

6 INCIDENT REPORTING FORMS

No local form has been developed to report incidents to CSIRT-INQUEST.
If possible, please provide the following information :

- Contact information, including electronic mail address and telephone number
- Date and time when the incident started
- Date and time when the incident was detected
- Incident description
- Affected assets, impact
- Actions taken so far

7 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, CSIRT-INQUEST assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.